JOURNAL OF INFORMATION SYSTEMS
Vol. 33, No. 3
Fall 2019
pp. A1–A2

American Accounting Association
DOI: 10.2308/isys-10715

EDITORIAL

Implications of Cybersecurity on Accounting Information

I. INTRODUCTION

Recent high-profile cybersecurity incidents, such as Equifax, Sony, and Target, have increased professional and regulatory attention. For example, organizations are under pressure to demonstrate that they are managing cybersecurity threats, and that they have effective processes and controls in place to detect, respond to, mitigate, and recover from breaches and other security events. Cybersecurity risk management involves not only improving internal controls, but also includes a wide range of factors from strategy, IT management, investment decisions, human behavior, disaster recovery/business continuity, and technical solutions to actual implementation and practices.

From the regulatory perspective, the PCAOB explicitly included the assessment of cybersecurity risks in its 2018–2022 strategic plan (PCAOB 2018). Further, the Securities and Exchange Commission (SEC) recently issued reporting guidelines on cybersecurity risk disclosures (SEC 2018), while the AICPA proposed an assurance framework for auditors to use to evaluate an organization's cybersecurity risk management policies and procedures (AICPA 2017).

Accounting information systems (AIS) researchers, who stand at the intersection between information systems and accounting, can contribute to understanding the impact of cybersecurity on accounting information from different theoretical or empirical perspectives. For example, our emphasis on understanding how behavior impacts action may provide insight to managers as they develop and implement cybersecurity policies and work to prevent and detect cybersecurity breaches. Further, our knowledge of how financial and nonfinancial information impacts organizational value may be helpful to investigate how investors and auditors react to disclosed data security breaches. Finally, we offer this special-theme issue to encourage cybersecurity research by the broader accounting community. To illustrate, Banker and Feng (2019) and Richardson, Smith, and Watson (2019) demonstrate how archival financial methodology can be used to examine important cybersecurity issues. Accounting behavioral researchers are encouraged to follow the lead of Cheng and Walton (2019) and Frank, Grenier, and Pyzoha (2019) in using experiments to provide insights into cybersecurity challenges. Further, managerial researchers may find Curry, Marshall, Correia, and Crossler's (2019) work helpful in generating ideas on how applicable theories and skills can be applied to this important topic.

II. THEME ISSUE: IMPLICATIONS OF CYBERSECURITY

This special-theme issue presents seven papers that represent a variety of cybersecurity issues using several research methods and theories. The first paper examines breach detection. Specifically, O'Leary (2019) uses textual analysis to detect phishing, a growing cybersecurity incident problem. The paper proposes that the probability of an email to be a phishing incident increases depending upon who the fraudster is impersonating (i.e., friend), whether the email includes goal achievement, and whether the email included references to the victim's work. The paper presents models built using nominal regression and neural networks to demonstrate differences between phishing emails and Enron emails.

Cybersecurity experts often encourage individuals to engage in strong password controls. Curry et al. (2019), building on the InfoSec Process Action Model (IPAM), explore how nontechnical assessments and interventions can indicate and reduce the likelihood of risk individual behavior. Specifically, their multi-stage password-setting experiments show that the security compliance behavior can be predicted and demonstrate strategies that management can use to reduce the probability that employees engage in weak password behavior.

Two papers examine how managers react to data security breaches. Xu, Guo, Haislip, and Pinsker (2019) explore whether managers are more likely to engage in earnings management following detection of data security breaches. Their findings suggest that firms are more likely to engage in real earnings management when the breach is related to financial information, the disclosure of the breach is delayed and the information environment is weaker (measured by low analyst coverage). From a different perspective, Banker and Feng (2019) also examine how managers respond to detected data security breaches by examining the association between detected data security breaches and chief information officer (CIO) turnover. The authors argue that security breaches reflect the CIO's information technology (IT) performance. When the CIOs fail to meet this performance expectation (i.e., a breach occurs), the likelihood of turnover will increase. Their findings demonstrate that the breach increase CIO turnover likelihood by 72 percent.

The next study examines the economic impact of privacy breaches. Specifically, Richardson et al. (2019) explore whether data privacy breaches impact organizations' abnormal returns, future accounting measures of performance, insider sales, and

reporting of SOX Section 404 internal control material weaknesses. Results indicate that, on average, the economic consequences of privacy breaches on firms' cumulative abnormal returns, future accounting measures of performance such as sale growth return on sales and operating expense, higher audit and other fees, and future SOX 404 reports of material internal control weaknesses are generally very small.

Frank et al. (2019) examine whether a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. The authors design an experiment to capture how disclosures proposed by AICPA may influence nonprofessional investors' perceptions. The authors find that issuing a management's report without assurance is more effective when a company has not disclosed a prior cyberattack. Further, issuing an independent cybersecurity assurance report may increase a company's ability to attract investments.

Finally, Cheng and Walton (2019) explore whether the timing and source of data breaches impact investors' reactions to the data breaches. By using an experimental setting, the authors demonstrate that investors are less likely to invest in a company if the breach is announced by the company itself, as compared to an outside source. However, timeliness does not seem to be a major factor in whether investors will invest in a company with a data breach.

III. FUTURE RESEARCH DIRECTIONS

This special-theme issue is just one step in an extended process to examine how cybersecurity impacts accounting information. More work is needed to improve how data incidents and breaches are detected and to reduce the probability that data incidents and breaches occur. Further, management response to cybersecurity breaches requires additional exploration. While some studies have examined how investors react to cybersecurity breaches, more work in understanding investors, auditors, and regulators behavior would be helpful.

—Diane J. Janvrin
Iowa State University

—Tawei Wang
DePaul University

REFERENCES

American Institute of Certified Public Accountants (AICPA). 2017. *SOC for Cybersecurity: Helping You Build Trust and Transparency*. Durham, NC: AICPA. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-cybersecurity-brochure.pdf

Banker, R., and C. Feng. 2019. The impact of information security breach incidents on CIO turnover. *Journal of Information Systems* 33 (3): 309–329. https://doi.org/10.2308/isys-52532

Cheng, X., and S. Walton. 2019. Do nonprofessional investors care about how and when data breaches are disclosed? *Journal of Information Systems* 33 (3): 163–182. https://doi.org/10.2308/isys-52410

Curry, M., B. Marshall, J. Correia, and R. Crossler. 2019. InfoSec process action model (IPAM): Targeting insider's weak password behavior. *Journal of Information Systems* 33 (3): 201–225. https://doi.org/10.2308/isys-52381

Frank, M., J. Grenier, and J. Pyzoha. 2019. How prior cyberattacks influence the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems* 33 (3): 183–200. https://doi.org/10.2308/isys-52374

O'Leary, D. 2019. What phishing emails reveal: An exploratory analysis of phishing attempts using text analysis. *Journal of Information Systems* 33 (3): 285–307. https://doi.org/10.2308/isys-52481

Public Company Accounting Oversight Board (PCAOB). 2018. *Strategic plan 2018–2022*. Available at: https://pcaobus.org/About/Administration/Documents/Strategic%20Plans/PCAOB-2018-2022-Strategic-Plan.pdf.

Richardson, V., R. Smith, and M. Watson. 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems* 33 (3): 227–265. https://doi.org/10.2308/isys-52379

Securities and Exchange Commission (SEC). 2018. *Commission statement and guidance on public company cybersecurity disclosures*. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf

Xu, H., S. Guo, J. Z. Haislip, and R. E. Pinsker. 2019. Earnings management in firms with data security breaches. *Journal of Information Systems* 33 (3): 267–284. https://doi.org/10.2308/isys-52480